Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-27. (Canceled)

28. (Currently Amended) An encoding apparatus comprising:

a block cipher key section to be initialized with a block cipher key, having transformation units to transform the block cipher key into [[(]]a transformed block cipher key[[)]];

a data section coupled with the block cipher key section to be initialized with a random number, having transformation units to transform the random number based on the transformed block cipher key;

a stream cipher key section coupled with the block cipher key section to modify the block cipher key according to a stream cipher key to produce data bits to dynamically modify the random number into [[(]]a modified random number[[)]] in the data block section; and

a mapping section to receive the modified random number and the transformed block cipher key and generate a pseudo random bit sequence based on the modified random number and the transformed block cipher key.

29. (Previously Presented) An apparatus according to claim 28, wherein the block cipher key section further includes first, second, and third registers, to be collectively initialized with the block cipher key.

30. (Previously Presented) An apparatus according to claim 29, wherein the block cipher key section further includes substitution units coupled between an output of the first register and an input of the third register, to make at least a partial substitution to the content of the first register and store the substituted content in the third register.

31. (Previously Presented) An apparatus according to claim 29, wherein the block cipher key section further includes a linear transformation unit coupled between an output of the second register and an input of the first register and an output of the third register and an input of the second register, to produce a linearly transformed version of the content of the second and third registers, and store the linearly transformed versions in the first and second registers, respectively.

32. (Previously Presented) An apparatus according to claim 28, wherein the data section is initialized with plain text.

33. (Previously Presented) An apparatus according to claim 28, wherein the data section is initialized with derived random number Mi-1.

34. (Previously Presented) An apparatus according to claim 28, wherein the data section further includes fourth, fifth, and sixth registers, to be collectively initialized with the random number.

35. (Previously Presented) An apparatus according to claim 34, wherein the data section further includes substitution units coupled between an output of the fourth register and an input of the sixth register, to make at least a partial substitution to the content of the fourth register and store the substituted content in the sixth register.

36. (Previously Presented) An apparatus according to claim 34, wherein the data section further includes a linear transformation unit coupled between an output of the fifth register and an input of the fourth register and an output of the sixth register and an input of the fifth register, to produce a linearly transformed version of the content of the fifth and sixth registers, and store the linearly transformed versions in the fourth and fifth registers, respectively.

37. (Previously Presented) An apparatus according to claim 34, wherein the block cipher key section includes first, second, and third registers to be collectively initialized with the block cipher key, and wherein the mapping section comprises a plurality of logical gates coupled with a register in the block cipher key section and a register in the data section.

38. (Previously Presented) An apparatus according to claim 28, wherein the stream cipher key section further includes linear feedback shift registers (LFSRs) to generate a first, second, and third sequence of data bits, and a serial network of shuffle units to shuffle the third sequence of data bits using the first sequence of data bits and input bits and the second sequence of data bits and control bits to the serial network of shuffle units.

39. (Currently Amended) An apparatus comprising:

a first key section to be enabled in a stream cipher mode and disabled in a block cipher mode, and to selectively modify a cipher key into [[(]]a selectively modified cipher key[[)]];

a second key section to be coupled with the first key section in the stream cipher mode, and having a first, second, and third registers to be collectively initialized with the cipher key, and transformation units coupled with the first, second, and third registers to recursively transform the selectively modified cipher key into [[(]]a transformed selectively modified cipher key[[)]];

a data section coupled with the second key section, having a fourth, fifth, and sixth registers to be collectively initialized with a data bit sequence, and transformation units coupled with the fourth, fifth, and sixth registers to transform the data bit sequence into [[(]]a transformed data bit sequence[[)]] according to the transformed selectively modified cipher key; and

a mapping section coupled with the second key section and the data section to generate a pseudo random bit sequence with the transformed data bit sequence.

40. (Previously Presented) An apparatus according to claim 39, wherein the first key section further includes linear feedback shift registers (LFSRs) to generate a first, second, and third sequence of data bits, and a serial network of shuffle units to shuffle the third sequence of data bits using the first sequence of data bits and input bits and the second sequence of data bits and control bits to the serial network of shuffle units.

41. (Previously Presented) An apparatus according to claim 39, wherein the second key section further includes substitution units coupled between an output of the first register and an input of the third register, to make at least a partial substitution to the content of the first register and store the substituted content in the third register.

42. (Previously Presented) An apparatus according to claim 39, wherein the second key section further includes a linear transformation unit coupled between an output of the second register and an input of the first register and an output of the third register and an input of the second register, to produce a linearly transformed version of the content of the second and third registers, and store the linearly transformed versions in the first and second registers, respectively.

43. (Previously Presented) An apparatus according to claim 39, wherein the data section is initialized with plain text.

44. (Previously Presented) An apparatus according to claim 39, wherein the data section is initialized with derived random number Mi-1.

45. (Previously Presented) An apparatus according to claim 39, wherein the data section further includes substitution units coupled between an output of the fourth register and an input of the sixth register, to make at least a partial substitution to the content of the fourth register and store the substituted content in the sixth register.

46. (Previously Presented) An apparatus according to claim 39, wherein the data section further includes a linear transformation unit coupled between an output of the fifth register and an input of the fourth register and an output of the sixth register and an input of the fifth register, to produce a linearly transformed version of the content of the fifth and sixth registers, and store the linearly transformed versions in the fourth and fifth registers, respectively.

47. (Previously Presented) An apparatus according to claim 39, wherein the mapping section comprises a plurality of logical gates coupled with a register in the second key section and a register in the data section.